

552.239-70

the President under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 *et seq.*) or to facilitate recovery from terrorism or nuclear, biological, chemical, or radiological attack.

(b) If the Schedule Contractor accepts an order from an entity identified in paragraph (d) of the clause at 552.238-78, Scope of Contract (Eligible Ordering Activities)—Alternate I, the Contractor agrees to the following conditions—

(1) The ordering entity is responsible for all payments due the Contractor for the contract formed by acceptance of the order, without recourse to the agency of the U.S. Government, which awarded the Schedule contract.

(2) The Contractor is encouraged, but not obligated, to accept orders from such entities. The Contractor may, within 5 days of receipt of the order, decline to accept any order, for any reason. The Contractor shall decline the order using the same means as those used to place the order. The Contractor shall fulfill orders placed by such entities, which are not declined within the 5-day period.

(c) In accordance with clause 552.238-74, Industrial Funding Fee and Sales Reporting, the Contractor must report the quarterly dollar value of all sales under this contract. When submitting sales reports, the Contractor must report two dollar values for each Special Item Number—

(1) The dollar value for sales to entities identified in paragraph (a) of the clause at 552.238-78, Scope of Contract (Eligible Ordering Activities)—Alternate I; and

(2) The dollar value for sales to entities identified in paragraph (d) of clause 552.238-78, Alternate I.

(d) A listing of the Federal Supply Schedule contracts for the products and services available for disaster recovery purchasing is accessible in GSA's Schedules e-Library at Web site <http://www.gsaelibrary.gsa.gov>. Click on the link, "Disaster Recovery Purchasing, State and Local." The participating Contractors and the products and services available for disaster recovery purchasing will be labeled with the Disaster Recovery Purchasing icon.

(End of clause)

[72 FR 4654, Feb. 1, 2007]

552.239-70 Information Technology Security Plan and Security Authorization.

As prescribed in 539.7002(a), insert the following provision:

48 CFR Ch. 5 (10-1-11 Edition)**INFORMATION TECHNOLOGY SECURITY PLAN AND SECURITY AUTHORIZATION (JUN 2011)**

All offers/bids submitted in response to this solicitation must address the approach for completing the security plan and certification and security authorization requirements as required by the clause at 552.239-71, Security Requirements for Unclassified Information Technology Resources.

(End of provision)

[76 FR 34888, June 15, 2011]

552.239-71 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 539.7002(b), insert the following clause:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2011)

(a) *General.* The Contractor shall be responsible for information technology (IT) security, based on General Services Administration (GSA) risk assessments, for all systems connected to a GSA network or operated by the Contractor for GSA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to GSA's information that directly supports the mission of GSA, as indicated by GSA. The term information technology, as used in this clause, means any equipment, including telecommunications equipment that is used in the automatic acquisition, storage, manipulation, management, control, display, switching, interchange, transmission, or reception of data or information. This includes major applications as defined by OMB Circular A-130. Examples of tasks that require security provisions include:

(1) Hosting of GSA e-Government sites or other IT operations;

(2) Acquisition, transmission, or analysis of data owned by GSA with significant replacement cost should the Contractors copy be corrupted;

(3) Access to GSA major applications at a level beyond that granted the general public; e.g., bypassing a firewall; and

(4) Any new information technology systems acquired for operations within the GSA must comply with the requirements of HSPD-12 and OMB M-11-11. Usage of the credentials must be implemented in accordance with OMB policy and NIST guidelines (e.g., NIST SP 800-116). The system must operate within the GSA's access management environment. Exceptions must be requested in

writing and can only be granted by the GSA Senior Agency Information Security Officer.

(b) *IT Security Plan.* The Contractor shall develop, provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with applicable Federal laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures. GSA's Office of the Chief Information Officer issued "CIO IT Security Procedural Guide 09-48, Security Language for Information Technology Acquisitions Efforts," to provide IT security standards, policies and reporting requirements. This document is incorporated by reference in all solicitations and contracts or task orders where an information system is contractor owned and operated on behalf of the Federal Government. The guide can be accessed at <http://www.gsa.gov/portal/category/25690>. Specific security requirements not specified in "CIO IT Security Procedural Guide 09-48, Security Language for Information Technology Acquisitions Efforts" shall be provided by the requiring activity.

(c) *Submission of IT Security Plan.* Within 30 calendar days after contract award, the Contractor shall submit the IT Security Plan to the Contracting Officer and Contracting Officers Representative (COR) for acceptance. This plan shall be consistent with and further detail the approach contained in the contractor's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as accepted by the Contracting Officer and COR, shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

(d) *Submission of a Continuous Monitoring Plan.* The Contractor must develop a continuous monitoring strategy that includes:

- (1) A configuration management process for the information system and its constituent components;
- (2) A determination of the security impact of changes to the information system and environment of operation;
- (3) Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
- (4) Reporting the security state of the information system to appropriate GSA officials; and
- (5) All GSA general support systems and applications must implement continuous

monitoring activities in accordance with this guide and NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

(e) *Security authorization.* Within six (6) months after contract award, the Contractor shall submit written proof of IT security authorization for acceptance by the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. The security authorization must be in accordance with NIST Special Publication 800-37. This security authorization will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This security authorization, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document, and shall include a final security plan, a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan. The Contractor shall comply with the accepted security authorization documentation.

(f) *Annual verification.* On an annual basis, the Contractor shall submit verification to the Contracting Officer that the IT Security plan remains valid.

(g) *Warning notices.* The Contractor shall ensure that the following banners are displayed on all GSA systems (both public and private) operated by the Contractor prior to allowing anyone access to the system:

Government Warning

****WARNING**WARNING**WARNING****

Unauthorized access is a violation of U.S. law and General Services Administration policy, and may result in criminal or administrative penalties. Users shall not access other users or system files without proper authority. Absence of access controls IS NOT authorization for access! GSA information systems and related equipment are intended for communication, transmission, processing and storage of U.S. Government information. These systems and equipment are subject to monitoring by law enforcement and authorized Department officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in this system by law enforcement and authorized Department officials. Use of this system constitutes consent to such monitoring.

****WARNING**WARNING**WARNING****

(h) *Privacy Act notification.* The Contractor shall ensure that the following banner is displayed on all GSA systems that contain Privacy Act information operated by the Contractor prior to allowing anyone access to the system:

552.241-70,**48 CFR Ch. 5 (10-1-11 Edition)**

This system contains information protected under the provisions of the Privacy Act of 1974 (Pub. L. 93-579). Any privacy information displayed on the screen or printed shall be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to \$5,000, or both.

(i) *Privileged or limited privileges access.* Contractor personnel requiring privileged access or limited privileges access to systems operated by the Contractor for GSA or interconnected to a GSA network shall adhere to the specific contract security requirements contained within this contract and/or the Contract Security Classification Specification (DD Form 254).

(j) *Training.* The Contractor shall ensure that its employees performing under this contract receive annual IT security training in accordance with OMB Circular A-130, FISMA, and NIST requirements, as they may be amended from time to time during the term of this contract, with a specific emphasis on the rules of behavior.

(k) *Government access.* The Contractor shall afford the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract, regardless of the location. Access shall be provided to the extent required, in the Government's judgment, to conduct an IT inspection, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of GSA data or to the function of information technology systems operated on behalf of GSA, and to preserve evidence of computer crime. This information shall be available to GSA upon request.

(l) *Subcontracts.* The Contractor shall incorporate the substance of this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(m) *Notification regarding employees.* The Contractor shall immediately notify the Contracting Officer when an employee either begins or terminates employment when that employee has access to GSA information systems or data. If an employee's employment is terminated, for any reason, access to GSA's information systems or data shall be immediately disabled and the credentials used to access the information systems or data shall be immediately confiscated.

(n) *Termination.* Failure on the part of the Contractor to comply with the terms of this clause may result in termination of this contract.

(End of clause)

[76 FR 34888, June 15, 2011]

552.241-70, Availability of Funds for the Next Fiscal Year or Quarter.

As prescribed in 541.501, insert the clause 552.241-70, Availability of Funds for the Next Fiscal Year or Quarter, instead of FAR 52.232-19, in all utility acquisitions.

AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR OR QUARTER (AUG 2010)

Funds are not presently available for performance under this contract beyond _____. The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond _____, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

(End of clause)

[75 FR 48873, Aug. 12, 2010]

552.241-71 Disputes (Utility Contracts).

As prescribed in 541.501, insert clause 552.241-71, Disputes (Utility Contracts), in solicitations and contracts for utility services subject to the jurisdiction and regulation of a utility rate commission.

DISPUTES (UTILITY CONTRACTS) (AUG 2010)

The requirements of the Disputes clause at FAR 52.233-1 are supplemented to provide that matters involving the interpretation of tariffed retail rates, tariff rate schedules, and tariffed terms provided under this contract are subject to the jurisdiction and regulation of the utility rate commission having jurisdiction.

(End of clause)

[75 FR 48873, Aug. 12, 2010]

552.242-70 Status Report of Orders and Shipments.

As prescribed in 542.1107, insert the following clause: